



UNITED STATES PATENT AND TRADEMARK OFFICE

52
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/881,147	06/14/2001	Geoffrey Cooper	SECU0001CIP	9105
22862	7590	05/18/2005	EXAMINER	
GLENN PATENT GROUP 3475 EDISON WAY, SUITE L MENLO PARK, CA 94025			KIM, JUNG W	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 05/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/881,147

Applicant(s)

COOPER ET AL.

Examiner

Jung W. Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 April 2005.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-40 are pending.
2. Applicant amended claims 25 and 33 in the amendment filed on April 19, 2005.
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

4. The objection to claims 25 and 33 due to a misspelled word are withdrawn as the amendment overcomes the objections.

Response to Arguments

5. Applicant's arguments filed April 19, 2005 have been fully considered but they are not persuasive.
6. On pg 3, 2nd paragraph, applicant alleges:
The examiner stated that Vaid discloses "a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data" and cited Vaid's Figure 8 and Reference Nos. 808-811.
7. It is noted that no such statement was made in the 103(a) rejection of claim 1.
The rejection in the previous action and the rejection of claim 1 reiterated below

expressly argues that Vaid in view of Rogers suggest receiving and processing the policy specification file. (January 12, 2005, paragraph 6)

8. Applicant on pgs. 3-4 discloses both the referenced and relevant portions of the Vaid disclosure then argues on pg. 4, 2nd and 3rd paragraph:

Nowhere does Vail in the above or elsewhere teach or disclose "a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data." Applicant respectfully requests that the Examiner show where Vaid discloses assigning dispositions to network events.

Nowhere does Rogers teach or disclose "a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data."

Accordingly, in view of the above, neither prior art of reference alone or in combination teach, disclose, suggest, or motivate all claimed limitations of claims 1 and 13.

9. First, applicant's bald conclusion that Vail nor Rogers discloses "a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data", does not adequately respond why the pertinent portion does not suggest nor teach the particular limitation: there is no rational on the part of applicant's argument to form such a judgment.

10. Second, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642

Art Unit: 2132

F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). As indicated above, the limitation in question is rejected under the teaching of Vaid in view of Rogers.

11. Third, contrary to applicant's allegations, the limitation is covered by the disclosure of Vaid in combination with Rogers: packet or data flows are received and analyzed by means of classification, wherein classes are defined by the content of the packet, the source and destination of the data, the type of flow associated with the data, and other features; wherein measuring parameters of the classes are based on a policy or rule. From the classification step, a determining step is made whether or not to apply a policy based on the classification and predetermined settings. Vaid, fig. 8 and related text. This disclosure of Vaid anticipates the limitation of "receiving and processing processed network packet data to assign dispositions to network events contained in the network packet data". Roger discloses establishing a policy specification within a policy specification file and a policy monitoring component for receiving and processing the policy specification file. Roger, fig. 3, reference no. 24 and related text. Hence, the limitations are taught or suggested by the prior art of record.

12. In reply to applicant's argument that neither Vaid nor Rogers teaches or suggests, either alone or in combination, the amended limitations of claims 25 and 33 (Remarks, pg. 7, 1st full paragraph), examiner respectfully disagrees. Rogers discloses a method of implementing a policy system, wherein the security policy file is repeatedly

updated pending on real-time events. Rogers, col. 17:7-52. A further explanation of the Rogers disclosure is outlined below in relation to this limitation.

Claim Rejections - 35 USC § 103

13. Claims 1-40 rejected under 35 U.S.C. 103(a) as being unpatentable over Vaid et al. U.S. Patent No. 6,502,131 (hereinafter Vaid) in view of Rogers et al. U.S. Patent No. 5,557,747 (hereinafter Rogers).

14. As per claim 1, Vaid discloses a system for analyzing network traffic to use in performing network and security assessments by listening on a subject network, interpreting events, and taking action (see Vaid, col. 2:45-55; Figure 3), comprising:

- a. a policy specification (see Vaid, Figure 2, Reference Nos. 201,202,221);
- b. a network monitor processor for processing network packet data collected from the subject network (see Vaid, col. 17:12-22; 13:57-14:5); and
- c. a policy-monitoring component for receiving and processing the processed network packet data to assign dispositions to network events contained in the network packet data (see Vaid, Figure 8, Reference Nos. 808-811).

Vaid does not expressly disclose that the policy specification is on a file. However, rule based policies are typically listed on a file in the art. As an example, a policy server taught by Rogers, implements a rule-based policy file to define policies. See Rogers, Figure 3, Reference No. 24. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement the policy specification as a file since files

Art Unit: 2132

are the standard form in which directory managed information is stored on a computer.

The aforementioned covers the limitations of claim 1.

15. As per claim 2, Vaid covers a system as outlined above in the claim 1 rejection.

In addition, the policy-monitoring component further comprises:

- d. a parser for parsing the policy specification file (see Rogers, Figure 3, Reference No. 50);
- e. a policy engine for synthesizing the parsed policy specification file and the processed network packet data, and for performing the assign dispositions and level of severity to the network events contained in the network packet data (see Vaid, col. 14:6-32; 16:55-17:56); and
- f. a logger for logging and storing into an events database the synthesized information by the policy engine according to a logging policy file (see Vaid, col. 22:37-39; 27:55).

The aforementioned cover the limitations of claim 2.

16. As per claim 3, Vaid covers a system as outlined above in the claim 2 rejection.

In addition, the system further comprises a query mechanism for mining the stored data in the events database. See Vaid, col. 22:9-29; Figure 15. The aforementioned cover the limitations of claim 3.

17. As per claim 4, Vaid covers a system as outlined above in the claim 2 rejection. In addition, the system further comprises an alarm script component for generating alarms based on the level of severity of the network events. See Vaid, col. 27:52-55. The aforementioned cover the limitations of claim 4.

18. As per claim 5, Vaid covers a system as outlined above in the claim 2 rejection. In addition, the system further comprises means for the policy engine interpreting each protocol event and consulting the policy specification file as each protocol event is interpreted to ensure that an earliest determination of the disposition is reached. See Vaid, Figure 2, Reference No. 231, and related text. The aforementioned cover the limitations of claim 5.

19. As per claim 6, Vaid covers a system as outlined above in the claim 1 rejection. In addition, the collected network packet data is captured in a file or is streams-based. See Vaid, Figure 2, especially Reference Nos. 211, 227 and 229, and related text. The aforementioned cover the limitations of claim 6.

20. As per claim 7, Vaid covers a system as outlined above in the claim 1 rejection. In addition, the system further comprises a secure web server comprising a web server component and a report database for displaying reports online, the reports generated by the events database using a report script. See Vaid, Figures 9-15 and related text. The aforementioned cover the limitations of claim 7.

21. As per claim 8, Vaid covers a system as outlined above in the claim 1 rejection. In addition, the system further comprises a parser for generating an English description policy representation from the policy specification file. See Vaid, Figures 16-19 and related text; see Rogers, Figure 3. The aforementioned cover the limitations of claim 8.

22. As per claim 9, Vaid covers a system as outlined above in the claim 1 rejection. In addition, the network monitor processor is used in standalone mode (see Vaid, col. 10:12-13). The aforementioned cover the limitations of claim 9.

23. As per claim 10, Vaid covers a system as outlined above in the claim 1 rejection. In addition, the network monitor processor and the policy-monitoring component run on a same machine. See Vaid, col. 10:7-11. The aforementioned cover the limitations of claim 10.

24. As per claim 11, Vaid covers a system as outlined above in the claim 1 rejection. In addition, the system further comprises a policy generator for generating the policy specification file. See Vaid, Figures 16-19, see Rogers, Figure 3. The aforementioned cover the limitations of claim 11.

25. As per claim 12, Vaid covers a system as outlined above in the claim 1 rejection. Vaid does not teach encrypting the network packet data received by the policy

Art Unit: 2132

monitoring component. However, it is notoriously well-known in the art to encrypt network packet data to prevent interception and tampering of transmitted data.

Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to encrypt the network packet data to ensure the integrity of the system as necessary for a system that performs security assessments. The aforementioned cover the limitations of claim 12.

26. As per claims 13-24, they are method claims corresponding to claims 1-12 and they do not teach or define above the information claimed in claims 1-12. Therefore, claims 13-24 are rejected as being unpatentable over Vaid in view of Rogers for the same reasons set forth in claims 1-12.

27. As per claim 33, Vaid covers a system as outlined above and further includes a system for developing a network security policy for a network, the system comprising:

- g. means for creating an initial network security policy file (see Vaid, Figure 19; see Rogers, Figure 3);
- h. means for ensuring the initial network security policy file is uploaded to a machine on the network (see Rogers, Figure 3, Reference No. 43);
- i. means for running a network monitor on the machine to collect the network traffic (see Vaid, col. 17:12-21);

- j. means for the network monitor outputting the collected network traffic in an output file, and passing the output file to a policy monitor (see Vaid, col. 13:44-14:27; 17:12-32);
- k. means for the policy monitor analyzing the collected network traffic (see Vaid, Figure 8);
- l. means for storing the analyzed network traffic in a database (see Vaid, col. 13:57-14:5; Figure 19);
- m. means for examining the analyzed network traffic in the database by querying the database using a query tool (see Vaid, Figure 15); and
- n. means for modifying the initial network security policy file as needed; until a comprehensive and desired policy file is attained (see Vaid, Figures 15 and 19).

28. Vaid does not expressly teach means for repeating from the means for ensuring network security policy file is uploaded through the means for modifying the network security policy file until a comprehensive and desired policy file is attained. Rogers discloses repeatedly updating the system state due to changes to system attributes or conditions as a result of changes in the network system parameters being monitored, and/or due to changes in local variables caused by the results of actions or policies after completion or caused by changes reflected due to a submission of a action or policy. Rogers, 17:7-52. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to repeat from the means for ensuring network security policy file is uploaded through the means for modifying the network security policy file

Art Unit: 2132

until a comprehensive and desired policy file is attained, since it ensures a more secure system for developing a security policy by enabling a continuous adjustment to the security policy driven by real-time events. Rogers, 2:6-20.

The aforementioned cover the limitations of claim 33.

29. As per claim 34, Vaid covers a system as outlined above in the claim 33 rejection. In addition, the network machine is remote, and further comprising means for uploading the modified network security policy file to the remote network machine as needed. See Vaid, Figure 1, Reference No. 110; see Rogers, Figure 3, Reference No. 43. The aforementioned cover the limitations of claim 34.

30. As per claim 35, Vaid covers a system as outlined above in the claim 33 rejection. In addition, the system further comprises means for monitoring network traffic by using the attained comprehensive and desired policy file. See Vaid, Figures 9-15 and 19; see Rogers, Figure 3. The aforementioned cover the limitations of claim 35.

31. As per claim 36, Vaid covers a system as outlined above in the claim 35 rejection. In addition, means for monitoring traffic is on a continuous basis. See Vaid, col. 11:1-11. The aforementioned cover the limitations of claim 36.

32. As per claim 37, Vaid covers a system as outlined above in the claim 33 rejection. In addition, the system further comprises means for generating reports from

Art Unit: 2132

the database, and using the generated reports as input for further policy refinement and/or using the generated reports for continuously monitoring network traffic. See Vaid, Figures 15 and 19. The aforementioned cover the limitations of claim 37.

33. As per claim 38, Vaid covers a system as outlined above in the claim 37 rejection. In addition, means for encrypting the reports and sending the encrypted reports to a remote Web server is an obvious limitation. See claim 12 rejection. The aforementioned cover the limitations of claim 38.

34. As per claim 39, Vaid covers a system as outlined above in the claim 38 rejection. In addition, the system further comprises means for accessing the reports on the remote server in a user-friendly manner. See Vaid, Figures 9-15, and 19. The aforementioned cover the limitations of claim 39.

35. As per claim 40, Vaid covers a system as outlined above in the claim 33 rejection. In addition, the means for creating an initial network security policy file and the step of modifying the network security policy file as needed uses a policy generator tool. See Vaid, Figures 15 and 19; see Rogers, Figure 3. The aforementioned cover the limitations of claim 40.

36. As per claims 25-32, they are method claims corresponding to claims 33-40 and they do not teach or define above the information claimed in claims 33-40. Therefore,

claims 25-32 are rejected as being unpatentable over Vaid in view of Rogers for the same reasons set forth in claims 33-40.

Conclusion

37. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

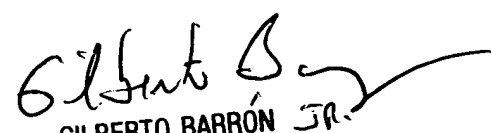
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
May 12, 2005



GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100